



FortiGate-AWS Deployment Guide



FortiGate-AWS Deployment Guide

September 25, 2014

01-500-252024-20140925

Copyright© 2014 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.

Technical Documentation	docs.fortinet.com
Knowledge Base	kb.fortinet.com
Customer Service & Support	support.fortinet.com
Training Services	training.fortinet.com
FortiGuard	fortiguard.com
Document Feedback	techdocs@fortinet.com

Table of Contents

I.	Overview	4
	Amazon Virtual Private Cloud (Amazon VPC)	
	Components of Amazon VPC	
	Network Information	
	Video Walk-through	
II.	Basic AWS Network Setup.....	7
	Step 1 – Setting up your AWS account	
	Step 2 – Create a Virtual Private Cloud (VPC)	
	Step 2.1 – VPC Wizard	
III.	FortiGate Provisioning	11
	Step 3 – EC2 Launching virtual machines	
	Step 3.1 – Choosing an AMI	
	Step 3.2 – Instance type	
	Step 3.3 – Instance Details	
	Step 3.4 – Instance Storage	
	Step 3.5 – Instance Tags	
	Step 3.6 – Security groups	
	Step 3.7 – Key Pair and Launch Instance	
IV.	Network Configuration	17
	Step 4 – Configure AWS network settings	
	Step 4.1 - Associate a public “elastic” IP to the FG-VM public interface	
	Step 4.2 – Confirm the assigned Public address	
	Step 4.3 – Setting up the default route for the private network.	
	Step 4.4 – Disable Source / Destination check on the Private FG interface.	
	Step 4.5 - Navigate to EC2 dash to review the Instance state	
	Step 4.6 - Access the Virtual FortiGate	
	Step 4.6 – SSH to the FortiGate	
V.	Step 5.0 – Setup a Test VM.....	24
	Step 5.1 – Provision a new AMI	
	Step 5.2 – Select a VM Instance type	
	Step 5.3 – Choose Instance settings	
	Step 5.4 – VM Storage settings	
	Step 5.5 – Assign any tags needed to the VM Instance	
	Step 5.6 – VM Security Group Settings	
	Step 5.7 – Review Instance Settings and Launch Instance	
	Step 5.8 – Create key pair	

VI.	Step 6.0 – FortiGate Configuration	30
	Step 6.1 - Update FortiGate Password	
	Step 6.2 – Confirm network settings	
	Step 6.3 – Setup basic policies	
VII.	Step 7 – Testing.....	33
	Step 7.1 – Launch a RDP session to test	
	Step 7.2 – Retrieve your VM’s password	
	Step 7.3 – Test Outbound access	
VIII.	Appendix.....	36
	Regions and Availability Zones	
	Amazon EC2 Key Pairs	
	Additional info and links	

Change History

Version	Date	Author.	Changes
1.0	8-1-2014	Justin L. Wireman	Initial Document creation

Overview

This document is design to be a quick start walk-through in setting up a virtual Fortinet device utilizing the AWS services. We will start out reviewing some of the AWS concepts.

Amazon Virtual Private Cloud (Amazon VPC)

Amazon VPC lets you provision a logically isolated section of the Amazon Web Services (AWS) Cloud where you can launch AWS resources in a virtual network that you define. You have complete control over your virtual networking environment, including selection of your own IP address range, creation of subnets, and configuration of route tables and network gateways. You can also create a Hardware Virtual Private Network (VPN) connection between your corporate datacenter and your VPC and leverage the AWS cloud as an extension of your corporate datacenter.

You can easily customize the network configuration for your Amazon VPC. For example, you can create a public-facing subnet for your web servers that have access to the Internet, and place your backend systems such as databases or application servers in a private-facing subnet with no Internet access. You can leverage multiple layers of security, including security groups and network access control lists, to help control access to Amazon EC2 instances in each subnet.

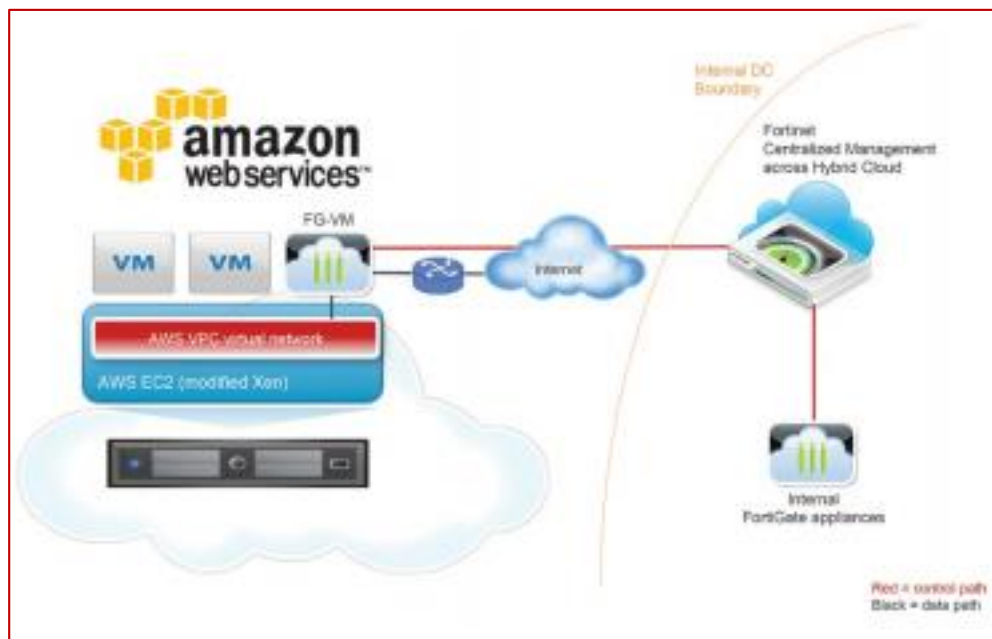


Figure 1

Components of Amazon VPC

Amazon VPC is comprised of a variety of objects that will be familiar to customers with existing networks:

- **A Virtual Private Cloud (VPC):** a logically isolated virtual network in the AWS cloud. You define a VPC's IP address space from a range you select.
- **Subnet:** a segment of a VPC's IP address range where you can place groups of isolated resources.
- **Internet Gateway:** the Amazon VPC side of a connection to the public Internet.
- **NAT Instance:** An EC2 instance that provides Port Address Translation for non-EIP instances to access the Internet via the Internet Gateway.
- **Hardware VPN Connection:** a hardware-based VPN connection between your Amazon VPC and your datacenter, home network, or co-location facility.
- **Virtual Private Gateway:** the Amazon VPC side of a VPN Connection.
- **Customer Gateway:** Your side of a VPN Connection.
- **Router:** Routers interconnect Subnets and direct traffic between Internet Gateways, Virtual Private Gateways, NAT instances and Subnets.
- **Peering Connection:** A peering connection enables you to route traffic via private IP addresses between two peered VPCs.

How do instances in a VPC access the Internet?

Elastic IP addresses (EIPs) give instances in the VPC the ability to both directly communicate outbound to the Internet and to receive unsolicited inbound traffic from the Internet (e.g., web servers)

How do instances without EIPs access the Internet?

Instances without EIPs can access the Internet in one of two ways:

Instances without EIPs can route their traffic through a NAT instance to access the Internet. These instances use the EIP of the NAT instance to traverse the Internet. The NAT instance allows outbound communication but doesn't enable machines on the Internet to initiate a connection to the privately addressed machines using NAT, and

For VPCs with a Hardware VPN connection, instances can route their Internet traffic down the Virtual Private Gateway to your existing datacenter. From there, it can access the Internet via your existing egress points and network security/monitoring devices.

Network Information

Figure #2 the default network design for a Public and Private VPC. We will be replacing much of the Router functionality with the FortiGate as pictured in figure 1.

- VPC Subnet – 10.0.0.0/16
- Public Subnet - 10.0.0.0/24
- Private Subnet – 10.0.1.0/24

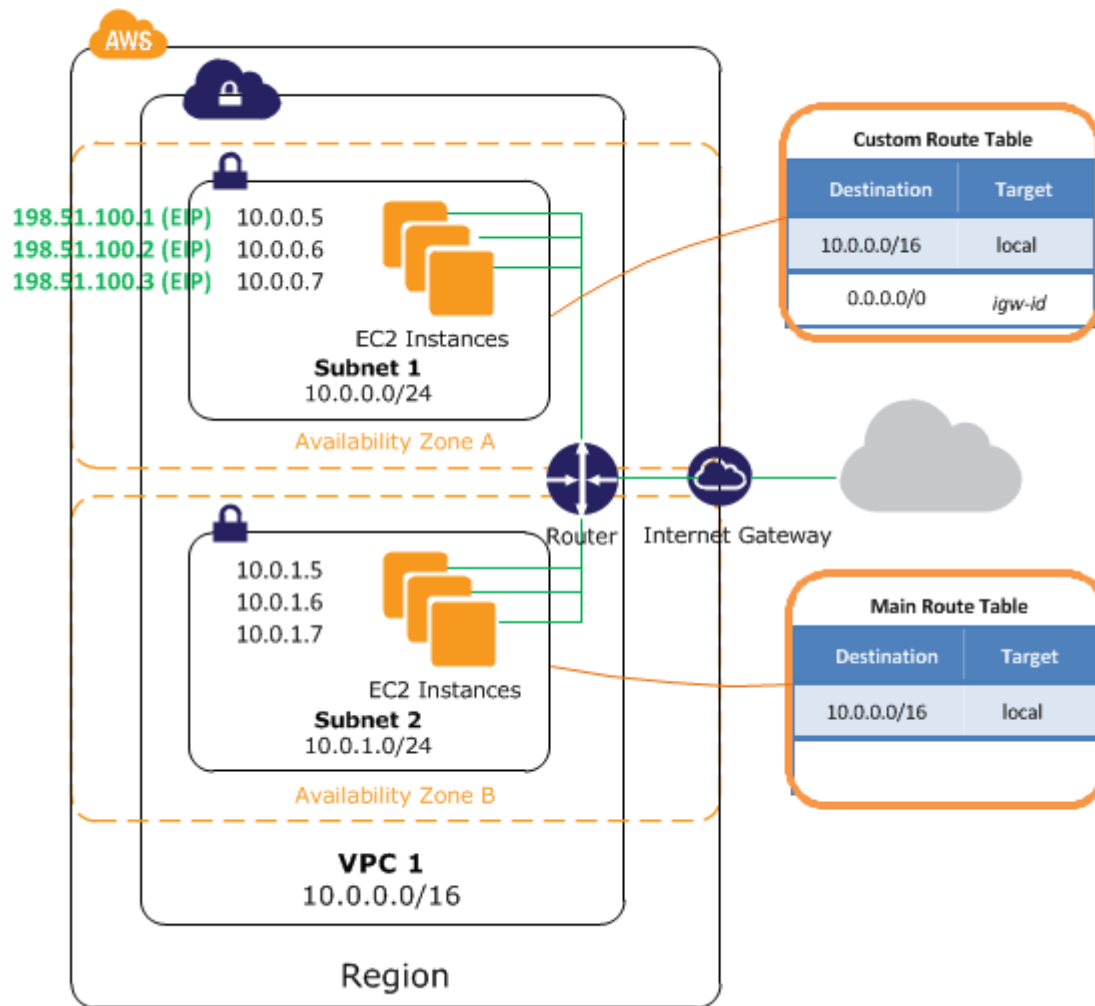


Figure 2 – Default Public / Private VPC design

Basic AWS Network Setup

Step 1 – Setting up your AWS account

For more information on AWS check out the getting started guide. [Click here](#)

You will need to provide billing information to setup an AWS account. Once you have completed the basic account setup you will be presented with the AWS console.

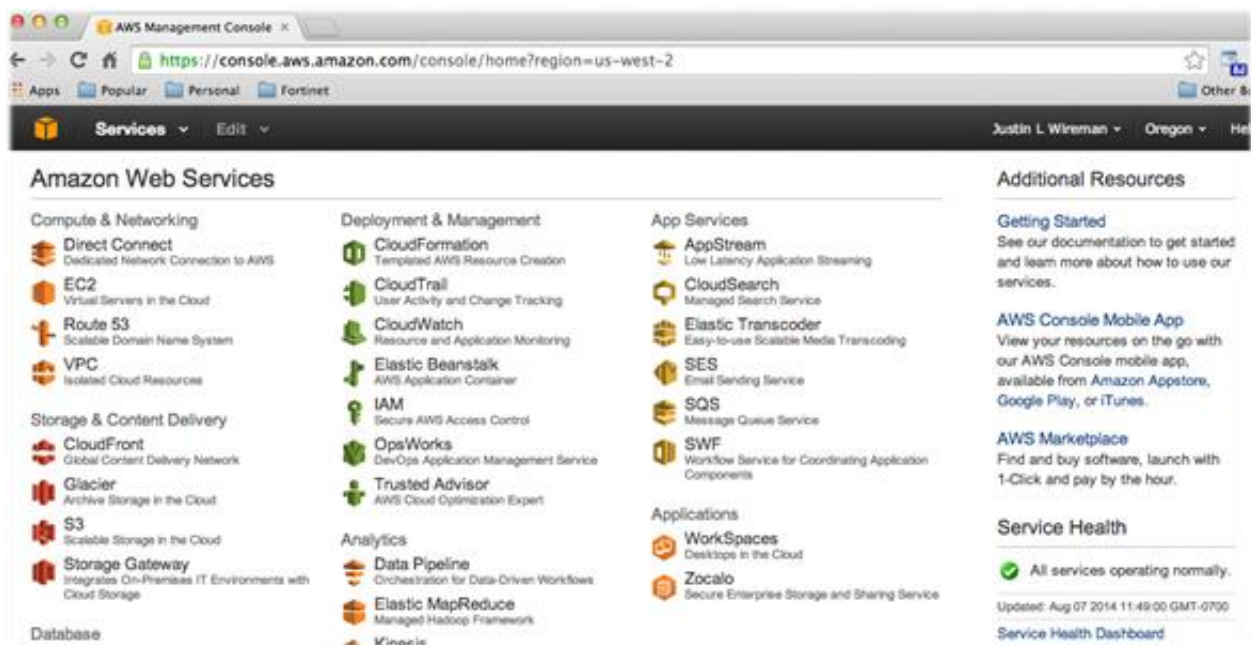


Figure 3

Step 2 – Create a Virtual Private Cloud (VPC)

To allow VM instances access to more than one interface you need to create a VPC (virtual private cloud). You need to change dashboards to VPC and for our purpose start the VPC wizard.

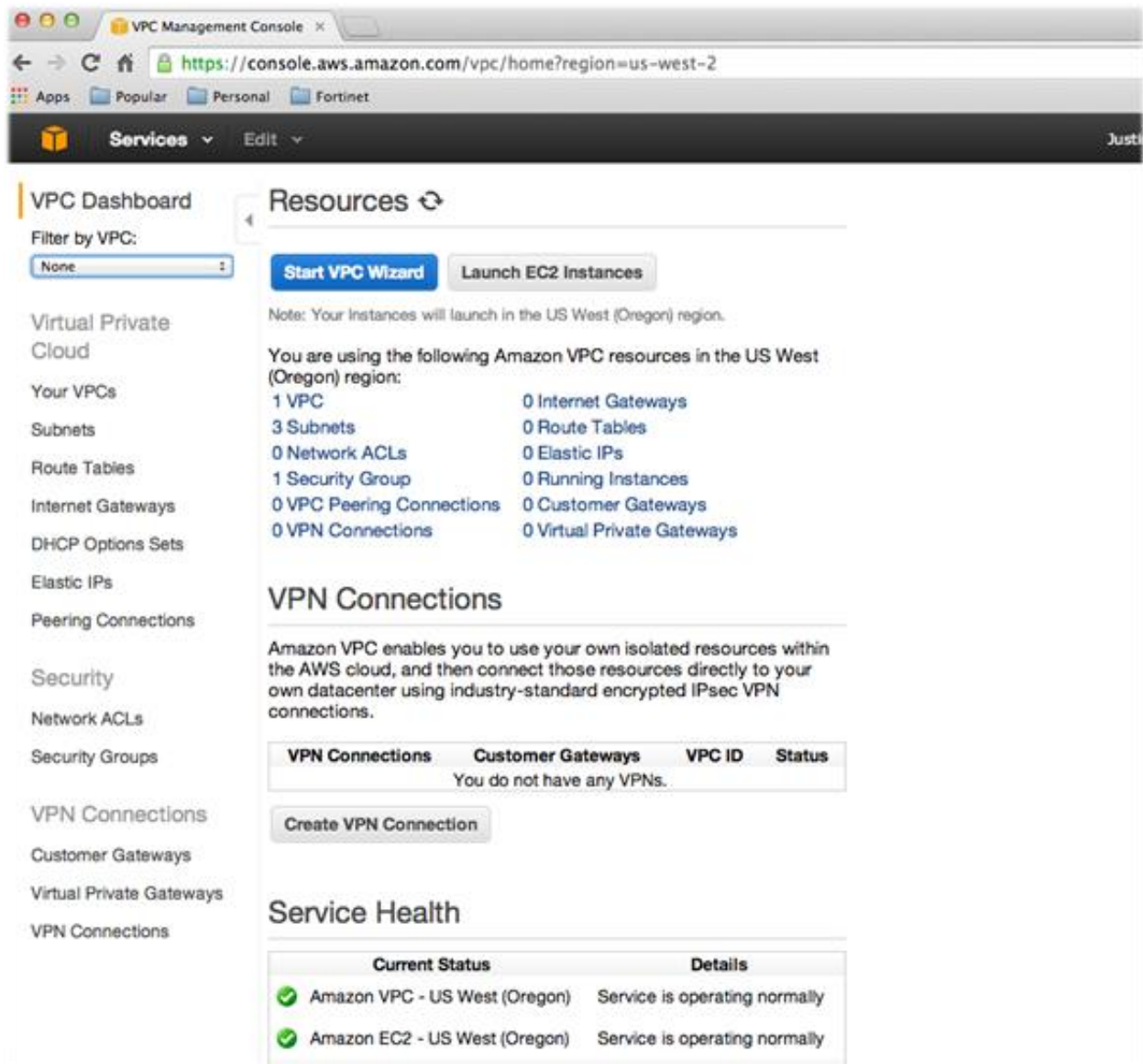


Figure 4 - VPC Dashboard

It is important to note that like most multi-tenant environments AWS reserves the first 5 IP address of each network that is created for its own router / firewall and DHCP / DNS servers.

Step 2.1 – VPC Wizard

This next section is a visual walk-through of the VPC wizard. Select the Public and Private subnet option.

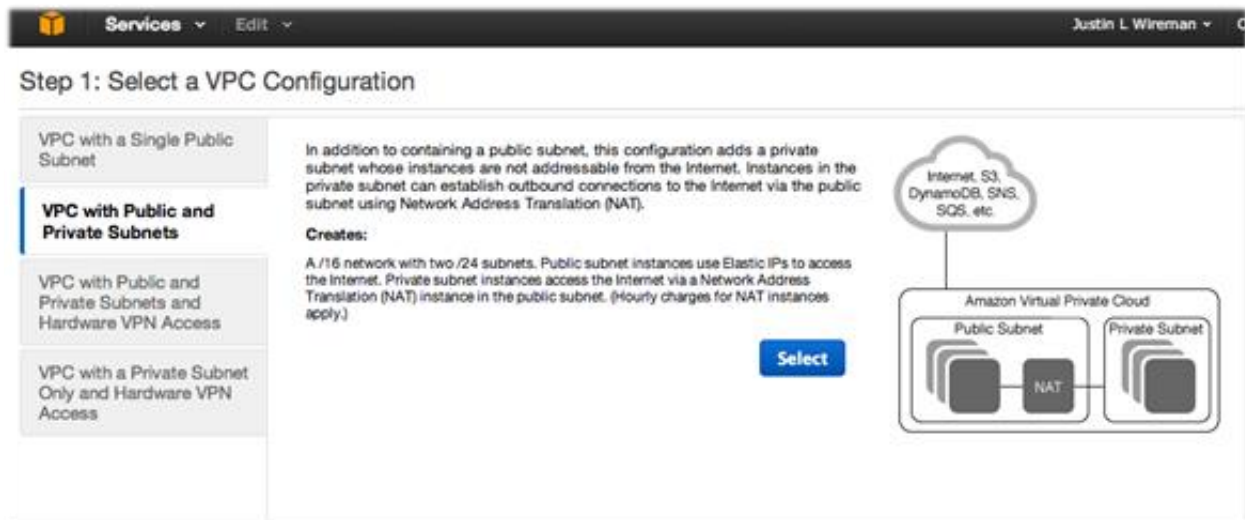


Figure 5 - VPC Wizard

One item to double check on step 2 of the VPC wizard is to make sure that both subnets are in the same availability zone. Please see the [Appendix](#) for more information on availability zones.

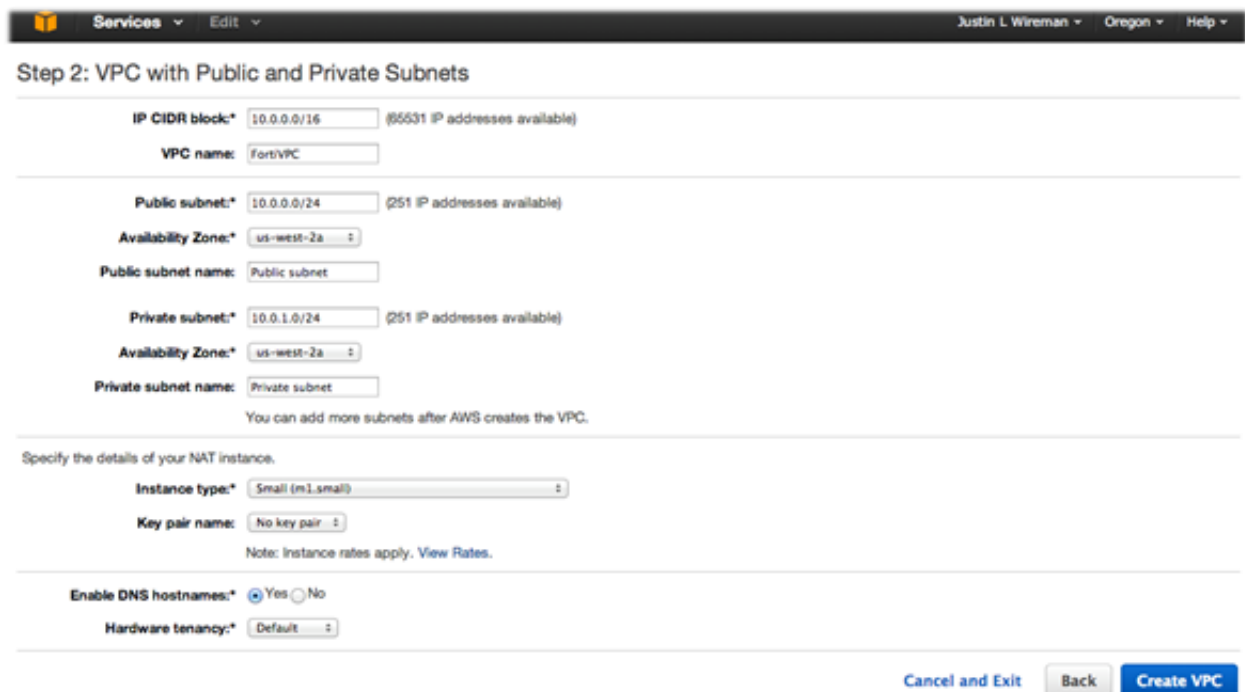


Figure 6 - VPC Wizard Subnets

Once you have verified the network setting, click create VPC and you will see the screen below.

Step 2: VPC with Public and Private Subnets

IP CIDR block: 10.0.0.0/16 (65531 IP addresses available)

VPC name: FortVPC

Public subnet: 10.0.0.0/24 (251 IP addresses available)

Availability Zone: us-west-2a

Public subnet name: Public subnet

Private subnet: 10.0.1.0/24 (251 IP addresses available)

Availability Zone: us-west-2a

Private subnet name: Private subnet

You can add more subnets after AWS creates the VPC.

Specify the details of your NAT instance.

Instance type: Small (m1.small)

Key pair name: No key pair

Note: Instance rates apply. View Rates.

Enable DNS hostnames: Yes (selected) No

Hardware tenancy: Default

Cancel and Exit Back Create VPC

Running NAT Instance (This may take a few minutes)...

57%

Figure 7 - VPC Wizard

When the VPC setup has been completed you can review subnet and routing information on the VPC Dashboard. More on this later in the guide, as you will need to alter settings to route traffic through the FortiGate.

VPC Dashboard

Filter by VPC: vpc-da4fb7bf (10.0.0.0/16)

Create Subnet Delete Subnet Modify Auto-Assign Public IP

Search Subnets and their properties

1 to 2 of 2 Subnets

	Name	Subnet ID	State	VPC	CIDR
<input type="checkbox"/>	Public subnet	subnet-81a571e4	available	vpc-da4fb7bf (10.0.0.0/16) ...	10.0.0.0/24
<input type="checkbox"/>	Private subnet	subnet-86a571e3	available	vpc-da4fb7bf (10.0.0.0/16) ...	10.0.1.0/24

Virtual Private Cloud

Your VPCs

Subnets

Route Tables

Internet Gateways

DHCP Options Sets

Elastic IPs

Peering Connections

Figure 8

FortiGate Provisioning

Step 3 – EC2 Launching virtual machines

Change dashboards to the EC2 dashboard. For time sake it is normally faster to get the VM provisioning started while setting up the network. Click Launch Instance on this screen.

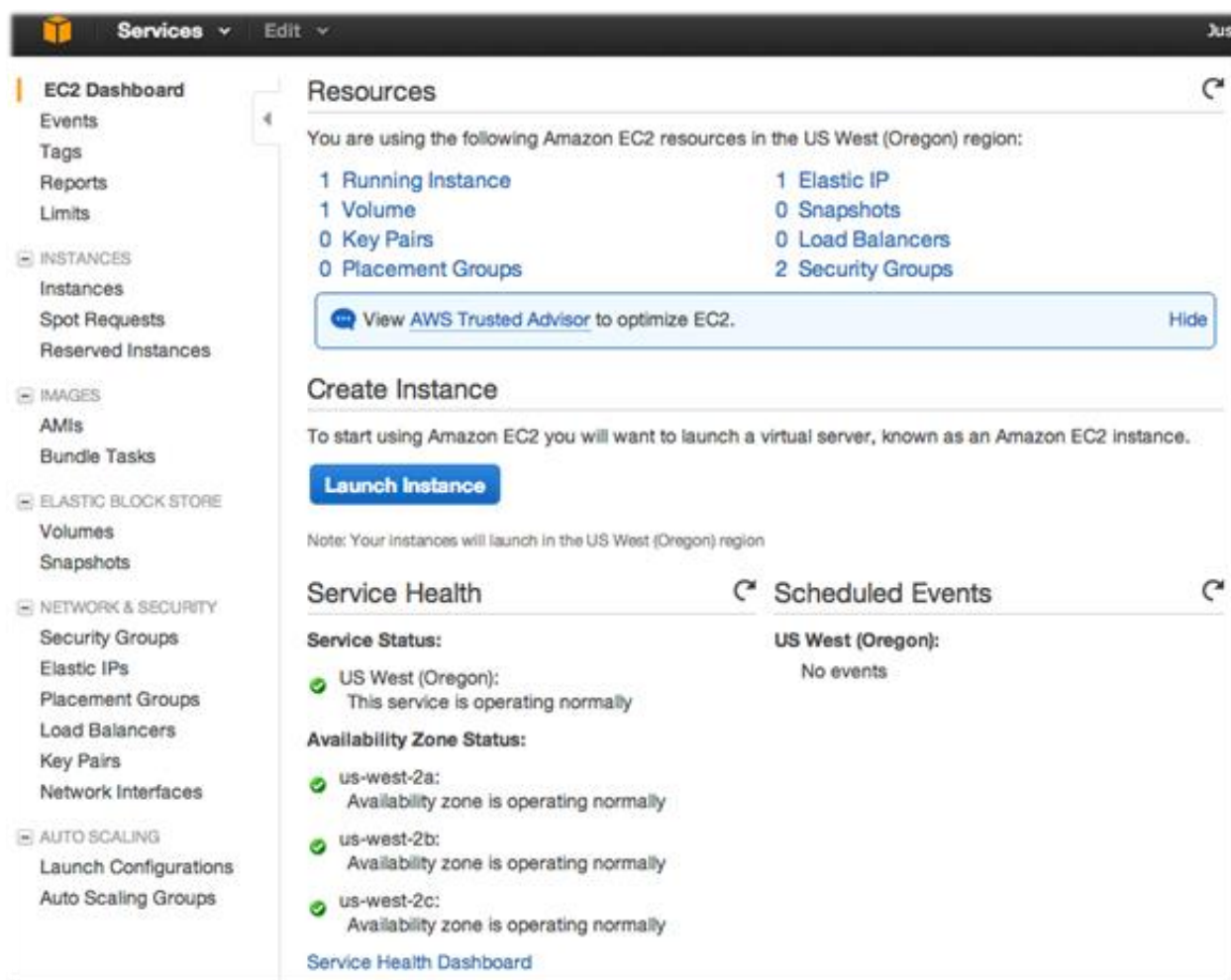


Figure 9 - EC2 Dashboard

Step 3.1 – Choosing an AMI

Services Edit Justin L. Wireman Oregon Help

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Tag Instance 6. Configure Security Group 7. Review

Step 1: Choose an Amazon Machine Image (AMI)

Cancel and Exit

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. You can select an AMI provided by AWS, our user community, or the AWS Marketplace; or you can select one of your own AMIs.

Quick Start My AMIs

AWS Marketplace Community AMIs

Categories All Categories Software Infrastructure (5)

Operating System Clear Filter All Linux/Unix Other Linux (5)

Software Pricing Plans Hourly (1) Annual (1) Bring Your Own License (4)

Region Current Region (5) All Regions (5)

Fortinet FortiGate-VM

★★★★★ (2) | v5.0.5 | Sold by Fortinet Inc.

Bring Your Own License + AWS usage fees

Linux/Unix, Other v5.0.5 | 64-bit Amazon Machine Image (AMI) | Updated: 3/3/14

FortiGate virtual appliances allow you to mitigate blind spots and improve policy compliance by implementing critical security controls within your virtual infrastructure ...

More info

Fortinet FortiAnalyzer-VM

★★★★★ (0) | v5.0.4 | Sold by Fortinet Inc.

Bring Your Own License + AWS usage fees

Linux/Unix, Other v5.0.4 | 64-bit Amazon Machine Image (AMI) | Updated: 11/10/13

FortiAnalyzer Network Security Logging, Analysis, and Reporting Appliances securely aggregate log data from Fortinet Security Appliances. A comprehensive suite of easily ...

More info

Fortinet FortiManager-VM

★★★★★ (0) | v5.0.4 | Sold by Fortinet Inc.

Bring Your Own License + AWS usage fees

Linux/Unix, Other v5.0.4 | 64-bit Amazon Machine Image (AMI) | Updated: 11/10/13

FortiManager Security Management appliances allow you to centrally manage any number of Fortinet Network Security devices, from several to thousands, including FortiGate, ...

More info

Figure 10 - AMI Wizard

For this guide we have chosen the Bring your Own License version of the FortiGate VM.

FortiGate-VM

Fortinet FortiGate-VM

FortiGate virtual appliances allow you to mitigate blind spots and improve policy compliance by implementing critical security controls within your virtual infrastructure. FortiGate virtual appliances include all of the security and networking services common to FortiGate physical appliances, giving you the freedom to deploy a centrally managed ...

Learn more on AWS Marketplace

Product Details

Sold by	Fortinet Inc.
Customer Rating	★★★★★ (2)
Latest Version	v5.0.5
Base Operating System	Linux/Unix, Other v5.0.5
Delivery Method	64-bit Amazon Machine Image (AMI)
License Agreement	End User License Agreement

Pricing Details

Bring Your Own License (BYOL)

Hourly Fees

Instance Type	Software	EC2	Total
C3 Large	\$0.00	\$0.105	\$0.105/hr
C3 Extra Large	\$0.00	\$0.21	\$0.21/hr
C3 Double Extra Large	\$0.00	\$0.42	\$0.42/hr
M3 Double Extra Large	\$0.00	\$0.56	\$0.56/hr
M3 Large	\$0.00	\$0.14	\$0.14/hr
M3 Extra Large	\$0.00	\$0.28	\$0.28/hr
M3 Medium	\$0.00	\$0.07	\$0.07/hr

EBS Storage Fees

\$0.10 / GB / Month for Standard EBS Storage


You will not be charged until you launch this instance.

Cancel Continue

Figure 11

Step 3.2 – Instance type

Choose the instance type that matches the license. For this example I have a 1 vCPU license file.

 **Services** ▼ Edit ▼ Justin L Wireman ▼ Oregon ▼ Help ▼

[1. Choose AMI](#) [2. Choose Instance Type](#) [3. Configure Instance](#) [4. Add Storage](#) [5. Tag Instance](#) [6. Configure Security Group](#) [7. Review](#)

Step 2: Choose an Instance Type

Amazon EC2 provides a wide selection of instance types optimized to fit different use cases. Instances are virtual servers that can run applications. They have varying combinations of CPU, memory, storage, and networking capacity, and give you the flexibility to choose the appropriate mix of resources for your applications. [Learn more](#) about instance types and how they can meet your computing needs.

Filter by: All instance types Current generation [Show/Hide Columns](#)

Currently selected: m3.medium (3 ECUs, 1 vCPUs, 2.5 GHz, Intel Xeon E5-2670v2, 3.75 GiB memory, 1 x 4 GiB Storage Capacity)

Note: The vendor recommends using a **m3.xlarge** instance (or larger) for the best experience with this product.

	Family	Type	vCPUs	Memory (GiB)	Instance Storage (GB)	EBS-Optimized Available	Network Performance
	General purpose	t2.micro Free tier eligible	1	1	EBS only	-	Low to Moderate
	General purpose	t2.small	1	2	EBS only	-	Low to Moderate
	General purpose	t2.medium	2	4	EBS only	-	Low to Moderate
<input checked="" type="checkbox"/>	General purpose	m3.medium	1	3.75	1 x 4 (SSD)	-	Moderate
<input type="checkbox"/>	General purpose	m3.large	2	7.5	1 x 32 (SSD)	-	Moderate
<input type="checkbox"/>	General purpose	m3.xlarge	4	15	2 x 40 (SSD)	Yes	High
<input type="checkbox"/>	General purpose	m3.2xlarge	8	30	2 x 80 (SSD)	Yes	High
<input type="checkbox"/>	Compute optimized	c3.large	2	3.75	2 x 16 (SSD)	-	Moderate
<input type="checkbox"/>	Compute optimized	c3.xlarge	4	7.5	2 x 40 (SSD)	Yes	Moderate
<input type="checkbox"/>	Compute optimized	c3.2xlarge	8	15	2 x 80 (SSD)	Yes	High

[Cancel](#) [Previous](#) [Review and Launch](#) [Next: Configure Instance Details](#)

Step 3.3 – Instance Details

In this step you will choose the public subnet, assign IP addresses, and add the eth1 interface (private subnet).

1. Choose AMI 2. Choose Instance Type **3. Configure Instance** 4. Add Storage 5. Tag Instance 6. Configure Security Group 7. Review

Step 3: Configure Instance Details

Number of instances ⓘ

Purchasing option ⓘ ☐ Request Spot Instances

Network ⓘ ⓘ [Create new VPC](#)

Subnet ⓘ ⓘ [Create new subnet](#)
250 IP Addresses available

Auto-assign Public IP ⓘ

IAM role ⓘ

Shutdown behavior ⓘ

Enable termination protection ⓘ ☐ Protect against accidental termination

Monitoring ⓘ ☐ Enable CloudWatch detailed monitoring
[Additional charges apply.](#)

Tenancy ⓘ ⓘ [Additional charges will apply for dedicated tenancy.](#)

▼ Network interfaces

Device	Network Interface	Subnet	Primary IP	Secondary IP addresses
eth0	<input type="text" value="New network interface"/>	<input type="text" value="subnet-81a571e4"/>	<input type="text" value="10.0.0.5"/>	Add IP
eth1	<input type="text" value="New network interface"/>	<input type="text" value="subnet-86a571e3"/>	<input type="text" value="10.0.1.5"/>	Add IP

[Cancel](#) [Previous](#) [Review and Launch](#)

Step 3.4 – Instance Storage

If you are configuring this for demonstration purposes, you can change the highlighted storage size to create a larger disk size for logging / reporting.

The screenshot shows the AWS Management Console interface for configuring an EC2 instance. The top navigation bar includes the AWS logo, 'Services' dropdown, 'Edit' dropdown, and the user name 'Justin L. Wireman'. Below the navigation bar is a progress bar with seven steps: 1. Choose AMI, 2. Choose Instance Type, 3. Configure Instance, 4. Add Storage (highlighted), 5. Tag Instance, 6. Configure Security Group, and 7. Review.

Step 4: Add Storage

Your instance will be launched with the following storage device settings. You can attach additional EBS volumes and instance store volumes to your instance, or edit the settings of the root volume. You can also attach additional EBS volumes after launching an instance, but not instance store volumes. [Learn more](#) about storage options in Amazon EC2.

Type	Device	Snapshot	Size (GiB)	Volume Type	IOPS	Delete on Termination	Encrypted
Root	/dev/sda1	snap-acbcb25d	2	General Purpose (SSD)	6 / 3000	<input type="checkbox"/>	Not Encrypted
EBS	/dev/sdb	Search (case-insensitive)	cb	Magnetic	N/A	<input checked="" type="checkbox"/>	<input type="checkbox"/>

[Add New Volume](#)

Free tier eligible customers can get up to 30 GB of EBS General Purpose (SSD) or Magnetic storage. [Learn more](#) about free usage tier eligibility and usage restrictions.

Figure 12

Step 3.5 – Instance Tags

It is valuable to create tags to quickly reference instance items in your AWS deployment. I have tagged a few items below as an example.

The screenshot shows the AWS Management Console interface for tagging an EC2 instance. The top navigation bar includes the AWS logo, 'Services' dropdown, 'Edit' dropdown, the user name 'Justin L. Wireman', the region 'Oregon', and a 'Help' dropdown. Below the navigation bar is a progress bar with seven steps: 1. Choose AMI, 2. Choose Instance Type, 3. Configure Instance, 4. Add Storage, 5. Tag Instance (highlighted), 6. Configure Security Group, and 7. Review.

Step 5: Tag Instance

A tag consists of a case-sensitive key-value pair. For example, you could define a tag with key = Name and value = Webserver. [Learn more](#) about tagging your Amazon EC2 resources.

Key (127 characters maximum)	Value (255 characters maximum)
Name	FortiGate-VM
Public IP	10.0.0.5
Private IP	10.0.1.5

[Create Tag](#) (Up to 10 tags maximum)

Figure 13 - Instance Tags

Step 3.6 – Security groups

Amazon by default has your VPC behind a basic firewall. Since we are going to be utilizing the FortiGate, I have created a Permit All security group and applied it to this instance.

Step 6: Configure Security Group

A security group is a set of firewall rules that control the traffic for your instance. On this page, you can add rules to allow specific traffic to reach your instance. For example, if you want to set up a web server and allow Internet traffic to reach your instance, add rules that allow unrestricted access to the HTTP and HTTPS ports. You can create a new security group or select from an existing one below. [Learn more](#) about Amazon EC2 security groups.

Assign a security group: ☒ Create a new security group ☐ Select an existing security group

Security group name:

Description:

Type	Protocol	Port Range	Source
All traffic	All	0 - 65535	Anywhere

Add Rule

Warning

Rules with source of 0.0.0.0/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.

Figure 14 - Security Groups

Step 3.7 – Key Pair and Launch Instance

- Choose proceed without a keypair and use the default FortiGate username / password.
- Click Launch Instance to begin the provisioning.

Step 7: Review Instance Launch

FortiGate-VM64-AWS build0202 Release

Root Device Type: sbs Virtualization type: hvm

Hourly Software Fees: \$0.00 per hour on m3.medium instance

Software charges

By launching this instance, you agree to the [Amazon EC2 End User License Agreement](#) and the seller's [terms and conditions](#).

Instance Type

Instance Type: EC2

m3.medium 3

Security Groups

Security group name: PermitAll

Description: This security group was generated by AWS Marketplace and is based on recommended settings

Type: All traffic

Protocol: All

Port Range: 0 - 65535

Source: 0.0.0.0/0

Select an existing key pair or create a new key pair

A key pair consists of a **public key** that AWS stores, and a **private key file** that you store. Together, they allow you to connect to your instance securely. For Windows AMIs, the private key file is required to obtain the password used to log into your instance. For Linux AMIs, the private key file allows you to securely SSH into your instance.

Note: The selected key pair will be added to the set of keys authorized for this instance. Learn more about [removing existing key pairs from a public AMI](#).

☒ I acknowledge that I will not be able to connect to this instance unless I already know the password built into this AMI.

Instance Details

Storage

Tags

Figure 15

Network Configuration

Step 4 – Configure AWS network settings

In this section you will be locating items such as the Network interface ENI on the EC2 dashboard and making IP and routing updates on the VPC dashboard.

Step 4.1 - Associate a public “elastic” IP to the FG-VM public interface

- On the EC2 Dashboard under the Network interface menu.
 - Locate the public interface ENI.
 - See step 4.3 figure 18 for a screenshot of this menu.
- On the VPC Dashboard under the Elastic IPs menu.
 - If the Public IP is associated with a default instance you will need to disassociate the Public IP before you can proceed.
 - Use the ENI of the public FortiGate interface as the object to associate the public IP.

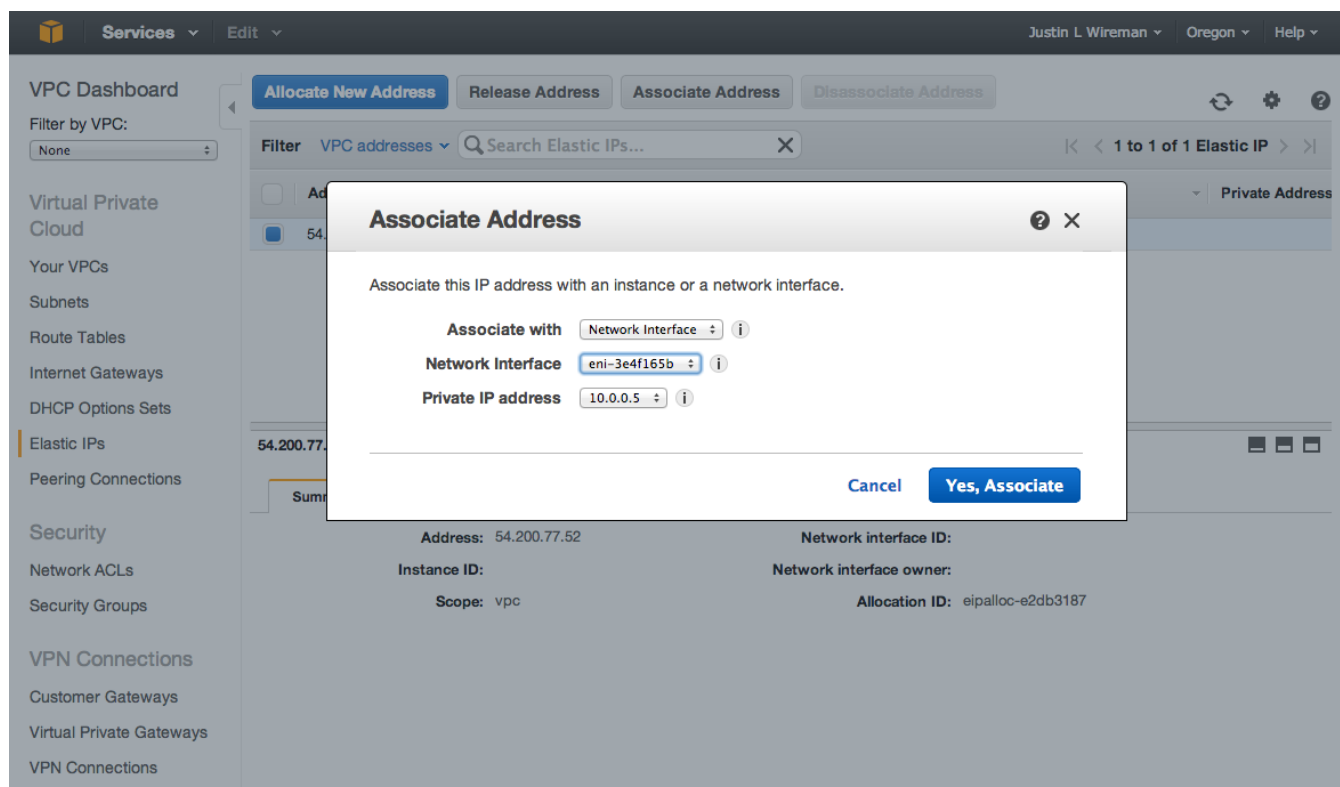


Figure 16

Step 4.2 – Confirm the assigned Public address

- Take note of the public IP address and DNS assigned. You will use these items in later steps.

The screenshot shows the AWS Management Console interface. On the left is a navigation menu with categories like INSTANCES, IMAGES, ELASTIC BLOCK STORE, NETWORK & SECURITY, and AUTO SCALING. The 'Elastic IPs' option under NETWORK & SECURITY is selected. The main content area displays a table of Elastic IP addresses. One address, 54.200.77.52, is selected. Below the table, a detailed view for this address is shown, including its public IP, instance (i-64fb846f), scope (vpc), and public DNS (ec2-54-200-77-52.us-west-2.compute.amazonaws.com). It also lists the network interface ID (eni-3e4f165b), private IP address (10.0.0.5), network interface owner (138006460020), and allocation ID (eipalloc-e2db3187).

Address	Instance	Private IP Address	Scope	Public DNS
54.200.77.52	i-64fb846f (FortiGate-VM)	10.0.0.5	vpc-da4fb7bf	ec2-54-200-77-52.u

Address: 54.200.77.52	
Public IP	54.200.77.52
Instance	i-64fb846f (FortiGate-VM)
Scope	vpc
Public DNS	ec2-54-200-77-52.us-west-2.compute.amazonaws.com
Network interface ID	eni-3e4f165b
Private IP address	10.0.0.5
Network interface owner	138006460020
Allocation ID	eipalloc-e2db3187

Figure 17

Step 4.3 – Setting up the default route for the private network.

- On the EC2 Dashboard under the Network interface menu.
 - Locate the network interface ID (ENI-) of the private network and Copy the ID.
- Change dashboards back to the VPC>Route Tables
 - Edit the default route (for the private subnet) to point to the FortiGate private network interface ID.
 - Demonstrated in figures 19-20

The screenshot shows the AWS Management Console's Network Interfaces page. The left sidebar lists various services, with 'Network Interfaces' highlighted under the 'NETWORK & SECURITY' section. The main content area displays a table of network interfaces. The interface 'eni-91752cf4' is selected, and its details are shown below the table.

Name	Network interface	Subnet ID	VPC ID	Zone	Security groups	Description	Instance ID
	eni-96752cf3	subnet-43ad7926	vpc-0e46be6b	us-west-2a	PermitALL	Primary netwo...	i-6
	eni-00752c65	subnet-43ad7926	vpc-0e46be6b	us-west-2a	default		i-9
Private FG Interface	eni-91752cf4	subnet-40ad7925	vpc-0e46be6b	us-west-2a	PermitALL		i-6

Network Interface: eni-91752cf4

Figure 18

The screenshot shows the AWS Management Console's VPC Dashboard's Route Tables page. The left sidebar lists various services, with 'Route Tables' highlighted under the 'Virtual Private Cloud' section. The main content area displays a table of route tables. The route table 'rtb-4701c522' is selected, and its details are shown below the table.

Name	Route Table ID	Associated With	Main	VPC
	rtb-4601c523	1 Subnet	No	vpc-0e46be6b (1)
	rtb-4701c522	0 Subnets	Yes	vpc-0e46be6b (1)

rtb-4701c522

Summary Routes Subnet Associations Route Propagation Tags

Edit

Destination	Target	Status	Propagated
10.0.0.0/16	local	Active	No
0.0.0.0/0	eni-00752c65 / i-96d6a99d	Active	No

Figure 19

rtb-4701c522

Summary Routes Subnet Associations Route Propagation Tags

Cancel Save

Destination	Target	Status	Propagated	Remove
10.0.0.0/16	local	Active	No	
0.0.0.0/0	eni-91752cf4	Active	No	✗
	eni-91752cf4 Private FG Interface No results			✗

Add another route

Figure 20

- Associate the private subnet to the private routing entry you have been editing in the previous steps.

rtb-4701c522

Summary Routes Subnet Associations Route Propagation Tags

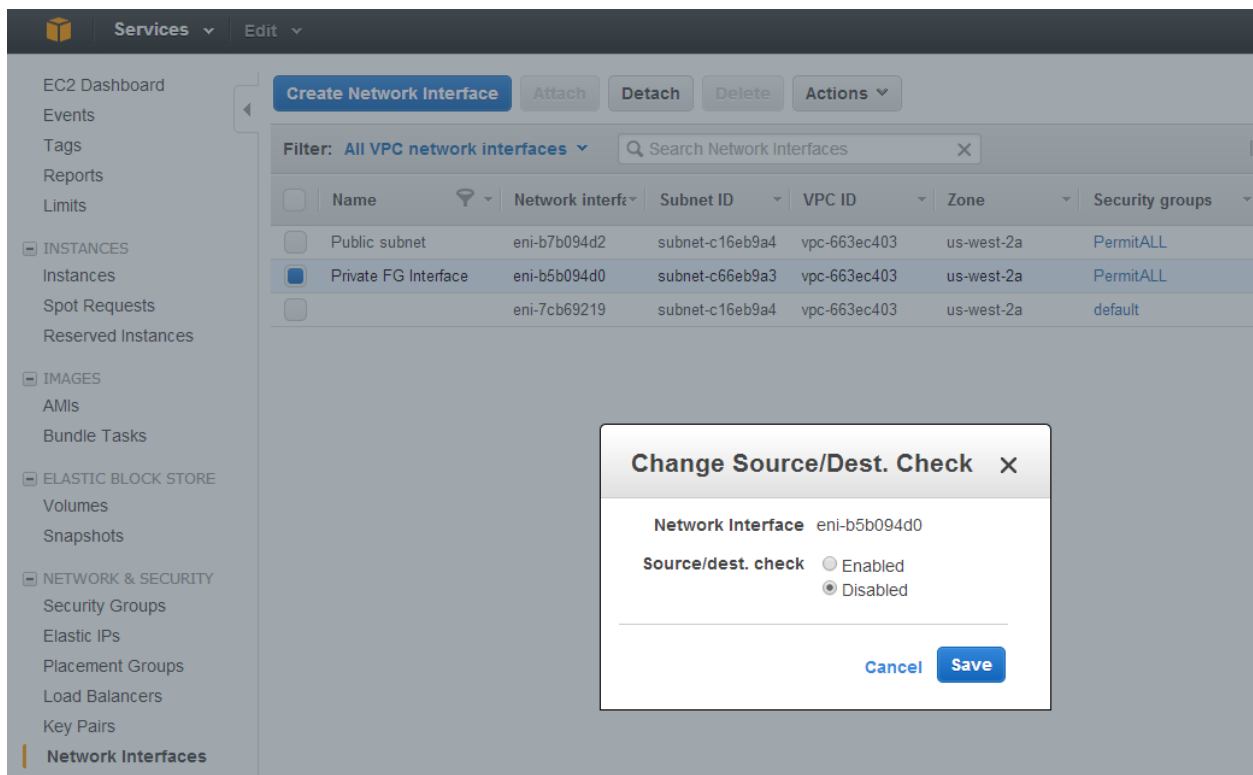
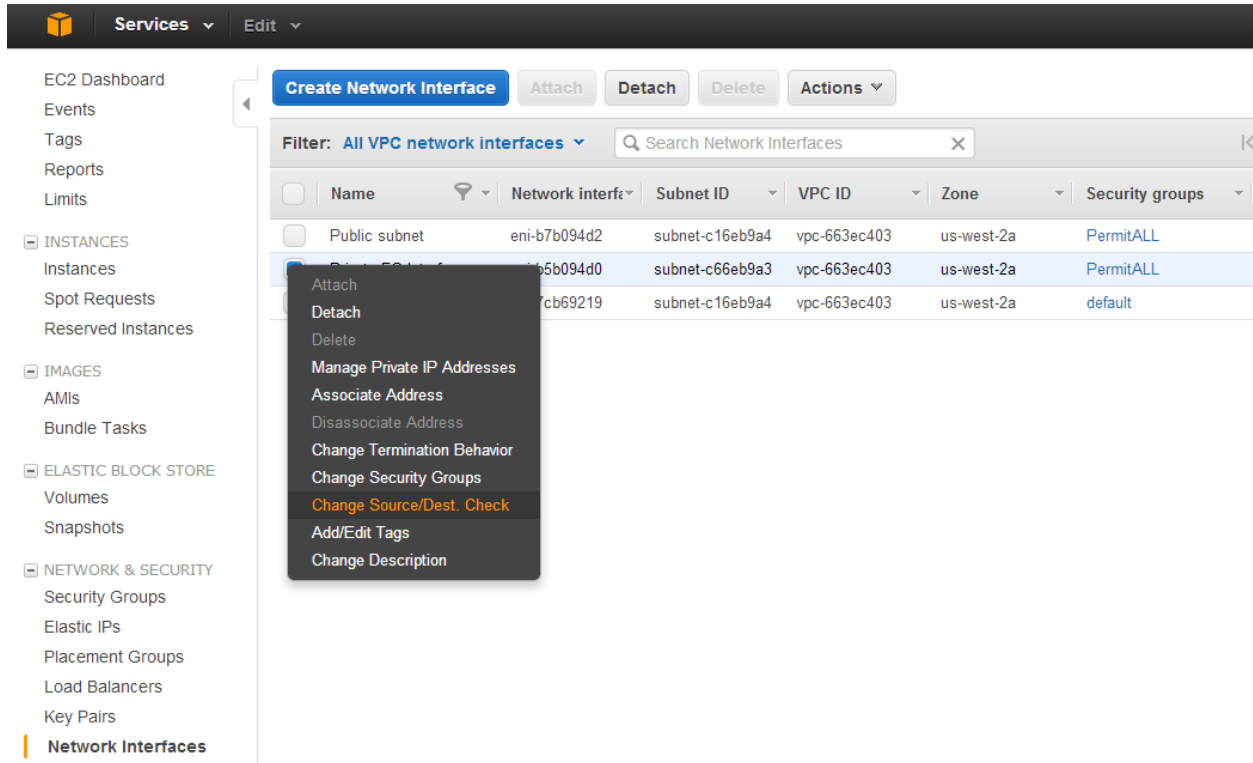
Cancel Save

Associate	Subnet	CIDR	Current Route Table
<input type="checkbox"/>	subnet-43ad7926 (10.0.0.0/24) Public subnet	10.0.0.0/24	rtb-4601c523
<input checked="" type="checkbox"/>	subnet-40ad7925 (10.0.1.0/24) Private subnet	10.0.1.0/24	Main

Figure 21

Step 4.4 – Disable Source / Destination check on the Private FG interface.

- On the EC2 Dashboard under the Network interface menu.
 - Right click and select Change Source/Dest Check
 - Select Disable and Save



Step 4.5 - Navigate to EC2 dash to review the Instance state

- Once confirming that the instance has finished provisioning and powering up check the following items.
 - Public IP/DNS assigned
 - Confirm the correct security group is assigned.

The screenshot shows the AWS Management Console interface. On the left is a navigation menu with categories like INSTANCES, IMAGES, ELASTIC BLOCK STORE, NETWORK & SECURITY, and AUTO SCALING. The main content area displays the details for an EC2 instance named 'FortiGate-VM' with ID 'i-64fb846f'. The instance is in the 'running' state and is located in the 'us-west-2a' availability zone. It has a public IP address of '54.200.77.52' and is associated with the 'PermitAll' security group. The instance was launched using the 'FortiGate-VM64-AWS build0252' AMI.

Instance ID	Instance state	Instance type	Private DNS	Private IPs	Secondary private IPs	VPC ID	Subnet ID	Network interfaces	Source/dest. check
i-64fb846f	running	m3.medium	ip-10-0-0-5.us-west-2.compute.internal	10.0.0.5		vpc-da4fb7bf	subnet-81a571e4	eth0 eth1	True

Public DNS	Public IP	Elastic IP	Availability zone	Security groups	Scheduled events	AMI ID	Platform	IAM role	Key pair name	Owner
ec2-54-200-77-52.us-west-2.compute.amazonaws.com	54.200.77.52	54.200.77.52	us-west-2a	PermitAll . view rules	No scheduled events	FortiGate-VM64-AWS build0252 AMI-e5936f4a-0d69-479f-919c-d5e158bd4d12-ami-5bd88032.2 (ami-f8026dc8)	-	-	-	138006460020

Step 4.6 - Access the Virtual FortiGate

- Open a HTTPS session to the public IP or DNS entry provided and login with the default username / password.
- Upload license file for BYOL. (See figure 22)
- The FortiGate will reboot after license install.

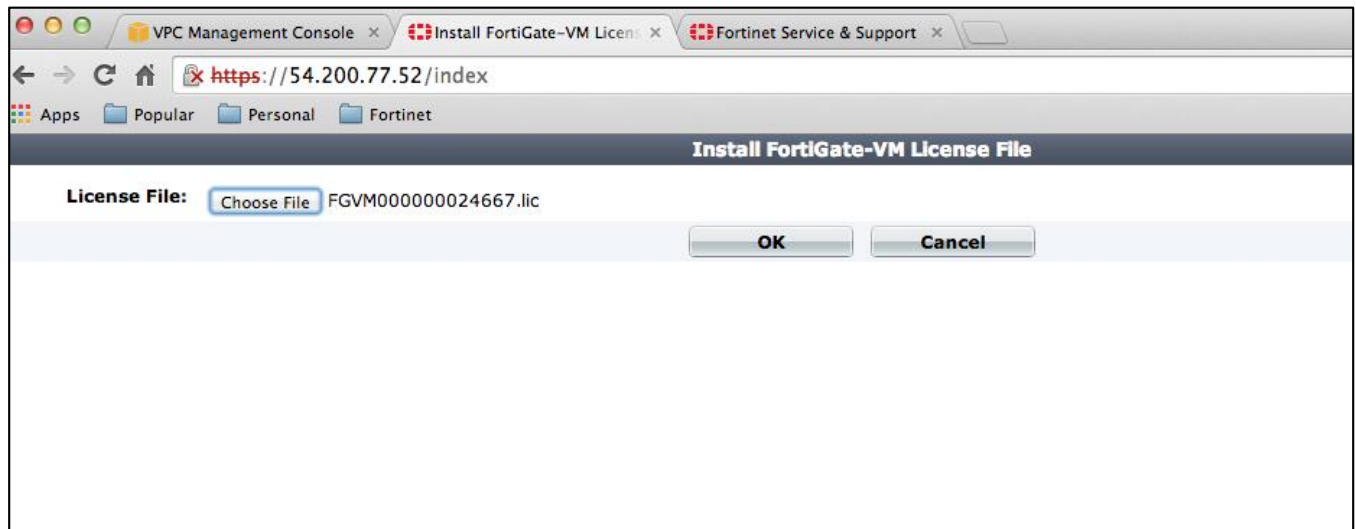


Figure 22

Step 4.7 – SSH to the FortiGate

- SSH to the device using the DNS hostname
- Issue the following commands to test access
 - Ping 8.8.8.8 to test connectivity
 - Execute update-now
 - Execute formatlogdisk and reboot (Option step if you need disk logging)

```
FortiGate-VM64-AWS# Execute ping 8.8.8.8
FortiGate-VM64-AWS# Execute update-now
FortiGate-VM64-AWS# Execute formatlogdisk
```


Step 5.0 – Setup a Test VM

In this step we will setup a test windows VM on the private network and configure it to use the FortiGate for all access in and out of the private network. In this example we are going to setup remote access to the test VM as well.

Step 5.1 – Provision a new AMI

For this example we are using Windows Server 2012. Note that any OS version could be used for testing / demonstration purposes.

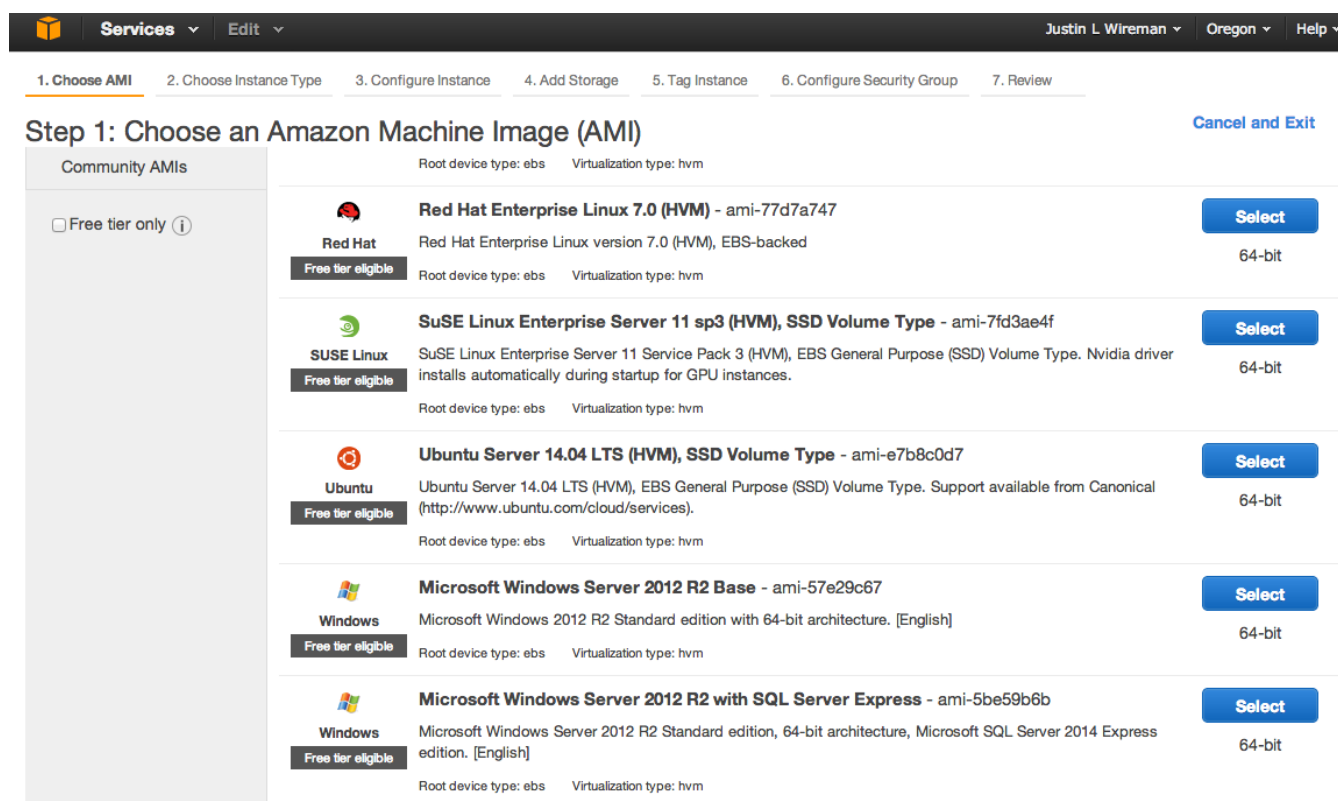


Figure 23

Step 5.2 – Select a VM Instance type

The default is the free tier general purpose type. This instance type is fine for basic testing.

Services Edit Justin L. Wireman Oregon Help

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Tag Instance 6. Configure Security Group 7. Review

Step 2: Choose an Instance Type

Amazon EC2 provides a wide selection of instance types optimized to fit different use cases. Instances are virtual servers that can run applications. They have varying combinations of CPU, memory, storage, and networking capacity, and give you the flexibility to choose the appropriate mix of resources for your applications. [Learn more](#) about instance types and how they can meet your computing needs.

Filter by: All instance types Current generation Show/Hide Columns

Currently selected: t2.micro (Variable ECUs, 1 vCPUs, 2.5 GHz, Intel Xeon Family, 1 GiB memory, EBS only)

	Family	Type	vCPUs	Memory (GiB)	Instance Storage (GB)	EBS-Optimized Available	Network Performance
<input checked="" type="checkbox"/>	General purpose	t2.micro Free tier eligible	1	1	EBS only	-	Low to Moderate
<input type="checkbox"/>	General purpose	t2.small	1	2	EBS only	-	Low to Moderate
<input type="checkbox"/>	General purpose	t2.medium	2	4	EBS only	-	Low to Moderate
<input type="checkbox"/>	General purpose	m3.medium	1	3.75	1 x 4 (SSD)	-	Moderate
<input type="checkbox"/>	General purpose	m3.large	2	7.5	1 x 32 (SSD)	-	Moderate
<input type="checkbox"/>	General purpose	m3.xlarge	4	15	2 x 40 (SSD)	Yes	High
<input type="checkbox"/>	General purpose	m3.2xlarge	8	30	2 x 80 (SSD)	Yes	High
<input type="checkbox"/>	Compute optimized	c3.large	2	3.75	2 x 16 (SSD)	-	Moderate
<input type="checkbox"/>	Compute optimized	c3.xlarge	4	7.5	2 x 40 (SSD)	Yes	Moderate
<input type="checkbox"/>	Compute optimized	c3.2xlarge	8	15	2 x 80 (SSD)	Yes	High
<input type="checkbox"/>	Compute optimized	c3.4xlarge	16	30	2 x 160 (SSD)	Yes	High

Cancel Previous Review and Launch Next: Configure Instance Details

Figure 24

Step 5.3 – Choose Instance settings

- It is important to select the private subnet to place this VM behind the FortiGate.
- I have also chosen to assign the IP address of 10.0.1.25. I have done this so I can setup port forwarding on the FortiGate while this VM is provisioned.

Services Edit Justin L Wireman Oregon Help

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Tag Instance 6. Configure Security Group 7. Review

Step 3: Configure Instance Details

number of instances 1

Purchasing option ☐ Request Spot Instances

Network vpc-da4fb7bf (10.0.0.0/16) | FortiVPC [Create new VPC](#)

Subnet subnet-86a571e3(10.0.1.0/24) | Private subnet | us-west-2 [Create new subnet](#)
250 IP Addresses available

Auto-assign Public IP Use subnet setting (Disable)

IAM role None

Shutdown behavior Stop

Enable termination protection ☐ Protect against accidental termination

Monitoring ☐ Enable CloudWatch detailed monitoring
[Additional charges apply.](#)

Tenancy Shared tenancy (multi-tenant hardware)
[Additional charges will apply for dedicated tenancy.](#)

▼ Network interfaces

Device	Network Interface	Subnet	Primary IP	Secondary IP addresses
eth0	New network interface	subnet-86a571e3	10.0.1.25	Add IP

[Add Device](#)

► Advanced Details

[Cancel](#) [Previous](#) [Review and Launch](#) [Next: Add Storage](#)

Figure 25

Step 5.4 – VM Storage settings

Adjust the default storage setting as appropriate for our virtual machine. If you are deploying this machine for basic testing the default should suffice.

The screenshot shows the 'Add Storage' step in the AWS Management Console. The top navigation bar includes 'Services' and 'Edit' dropdowns, and the user name 'Justin L Wireman'. The progress bar shows seven steps: 1. Choose AMI, 2. Choose Instance Type, 3. Configure Instance, 4. Add Storage (active), 5. Tag Instance, 6. Configure Security Group, and 7. Review.

Step 4: Add Storage

Your instance will be launched with the following storage device settings. You can attach additional EBS volumes and instance store volumes to your instance, or edit the settings of the root volume. You can also attach additional EBS volumes after launching an instance, but not instance store volumes. [Learn more](#) about storage options in Amazon EC2.

Type ⓘ	Device ⓘ	Snapshot ⓘ	Size (GiB) ⓘ	Volume Type ⓘ	IOPS ⓘ	Delete on Termination ⓘ	Encrypted ⓘ
Root	/dev/sda1	snap-435fe5b7	60	General Purpose (SSD) ▾	90 / 3000	<input checked="" type="checkbox"/>	Not Encrypted

[Add New Volume](#)

Free tier eligible customers can get up to 30 GB of EBS General Purpose (SSD) or Magnetic storage. [Learn more](#) about free usage tier eligibility and usage restrictions.

Figure 26

Step 5.5 – Assign any tags needed to the VM Instance

This is an optional step.

Step 5.6 – VM Security Group Settings

Assign the same “Permit All” security group you created during the step 3.6.

The screenshot shows the 'Configure Security Group' step in the AWS Management Console. The top navigation bar includes 'Services' and 'Edit' dropdowns, and the user name 'Justin L Wireman'. The progress bar shows seven steps: 1. Choose AMI, 2. Choose Instance Type, 3. Configure Instance, 4. Add Storage, 5. Tag Instance, 6. Configure Security Group (active), and 7. Review.

Step 6: Configure Security Group

A security group is a set of firewall rules that control the traffic for your instance. On this page, you can add rules to allow specific traffic to reach your instance. For example, if you want to set up a web server and allow Internet traffic to reach your instance, add rules that allow unrestricted access to the HTTP and HTTPS ports. You can create a new security group or select from an existing one below. [Learn more](#) about Amazon EC2 security groups.

Assign a security group: ☐ Create a new security group ☒ Select an existing security group

Security Group ID	Name	Description	Actions
<input type="checkbox"/> sg-636feb06	default	default VPC security group	Copy to new
<input checked="" type="checkbox"/> sg-4d69ed28	PermitAll	This security group was generated by AWS M...	Copy to new

Warning

Rules with source of 0.0.0.0/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.

Figure 27

Step 5.7 – Review Instance Settings and Launch Instance

Services

Edit

Justin L. Wireman

Oregon

Help

1. Choose AMI

2. Choose Instance Type

3. Configure Instance

4. Add Storage


5. Tag Instance

6. Configure Security Group

7. Review


Step 7: Review Instance Launch

Please review your instance launch details. You can go back to edit changes for each section. Click **Launch** to assign a key pair to your instance and complete the launch process.



Your instance configuration is not eligible for the free usage tier
To launch an instance that's eligible for the free usage tier, check your AMI selection, instance type, configuration options, or storage devices. Learn more about [free usage tier](#) eligibility and usage restrictions.


Don't show me this again



Improve your instance's security. Your security group, PermitAll, is open to the world.
Your instance may be accessible from any IP address. We recommend that you update your security group rules to allow access from known IP addresses only. You can also open additional ports in your security group to facilitate access to the application or service you're running, e.g., HTTP (80) for web servers. [Edit security groups](#)

AMI Details

Edit AMI



Microsoft Windows Server 2012 R2 Base - ami-57e29c67
Microsoft Windows 2012 R2 Standard edition with 64-bit architecture. [English]
Root Device Type: ebs Virtualization type: hvm

Free tier eligible

Instance Type

Edit instance type

Instance Type	ECUs	vCPUs	Memory (GiB)	Instance Storage (GB)	EBS-Optimized Available	Network Performance
t2.micro	Variable	1	1	EBS only	-	Low to Moderate

Security Groups

Edit security groups

Security	Name	Description
sg-4d69ed28	PermitAll	This security group was generated by AWS Marketplace and is based on recommended settings for FortiGate-VM version v5.0.5 provided by Fortinet

All selected security groups inbound rules

Cancel

Previous

Launch

Figure 28

Step 5.8 – Create key pair

If you already have a key pair you can use an existing one. If not choose to create a new key pair and download it. You will need this file to login to the VM.

Important - If you lose the key pair, you cannot connect to your Amazon EC2 instances.

For more information on Key Pairs see the Appendix

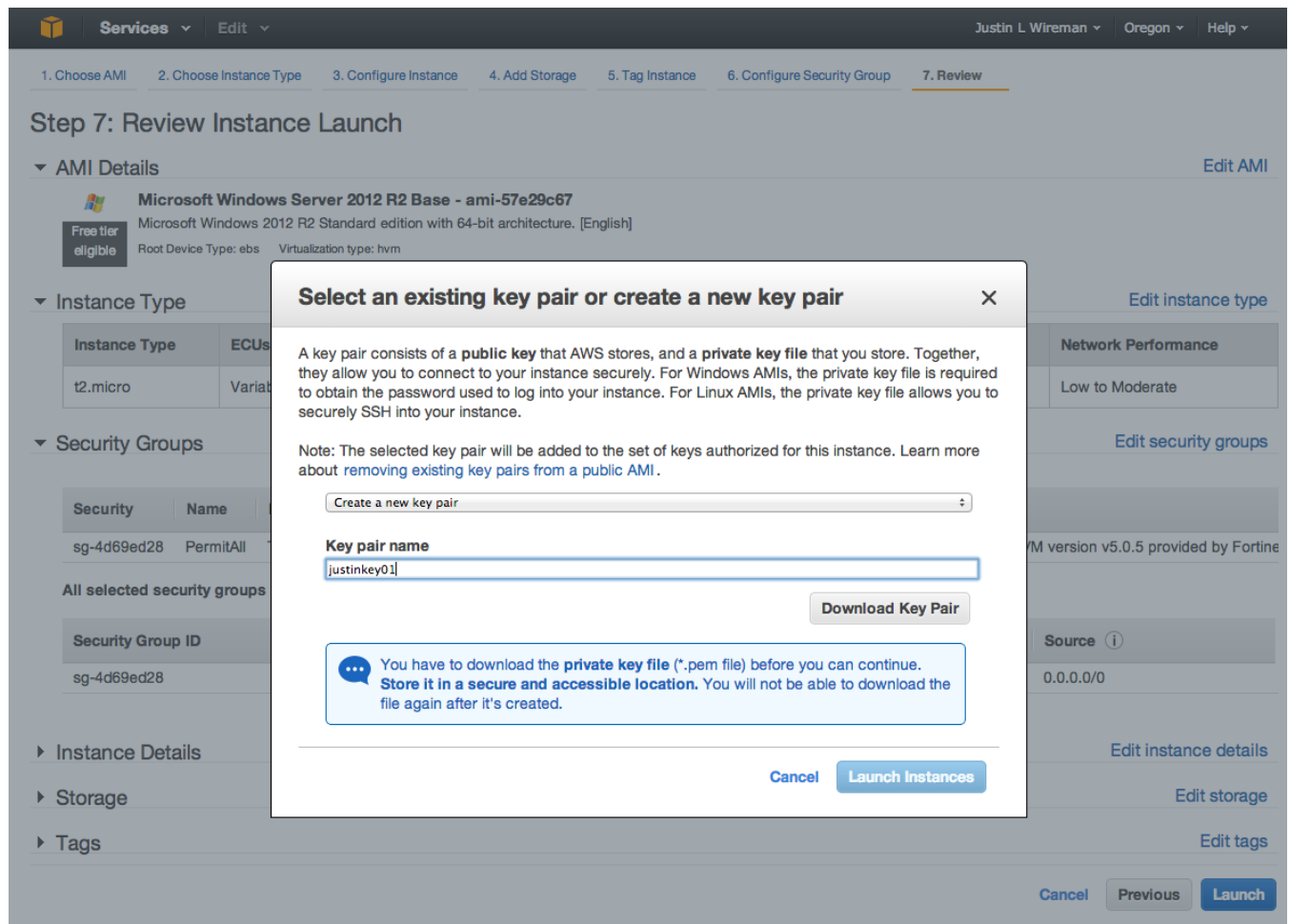


Figure 29 - Key Pair

Step 6.0 – FortiGate Configuration

While the Windows VM is being provisioned you can finish the FortiGate configuration.

Step 6.1 - Update FortiGate Password

Update the FortiGate password as there are many bots that attempt to log in to newly provisioned devices on AWS subnets.

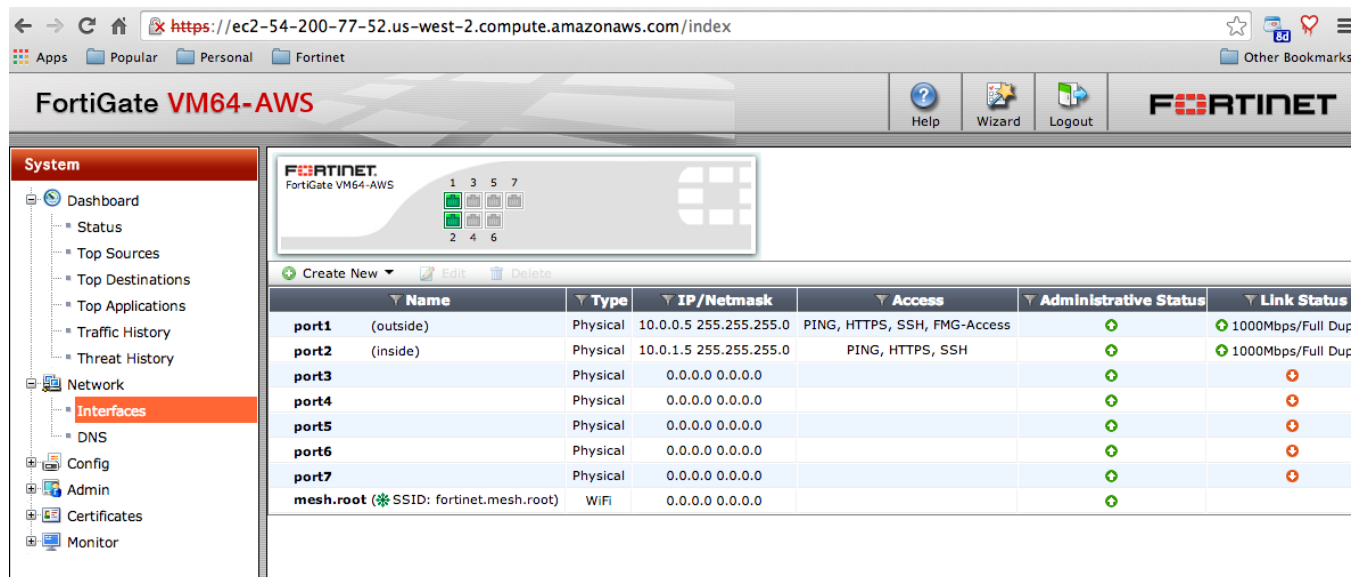
The screenshot displays the FortiGate VM64-AWS web interface. The left sidebar contains a navigation menu with categories like System, Network, Config, Admin, and Router. The main content area is divided into several panels:

- System Information:** Displays host details such as Host Name (ec2-54-200-77-52), Serial Number (FGVM000000024667), Operation Mode (NAT), HA Status (Standalone), System Time (Thu Aug 7 13:01:18 2014), Firmware Version (v5.0,build4348 (GA)), System Configuration ([Backup] [Restore] [Revisions]), Current Administrator (admin), Uptime (0 day(s) 0 hour(s) 7 min(s)), and Virtual Domain (Disabled).
- License Information:** Shows VM License (Registration Status: Valid), CPUs Detected (1 / 1), Support Contract (Registered), Firmware (8 x 5 support), and Enhanced Support (8 x 5 support).
- FortiGuard Services:** Lists services like Next Generation Firewall (IPS & Application Control), ATP Services (AntiVirus, Web Filtering), and Other Services (Vulnerability Scan, Email Filtering).
- System Resources:** Features two gauges for CPU Usage (0%) and Memory Usage (10%), along with Reboot and Shutdown buttons.
- Features:** A section for configuring various features, including Basic Features (Advanced Routing, IPv6, VPN, WAN Opt. & Cache, WiFi Controller) and Security Features (AntiVirus, Application Control, DLP, Email Filter, Endpoint Control, Explicit Proxy, Intrusion Protection, Vulnerability Scan, Web Filter).

Figure 30

Step 6.2 – Confirm network settings

Set the port2 interface IP address settings (private subnet)



The screenshot shows the FortiGate VM64-AWS web interface. The left sidebar contains a 'System' menu with options like Dashboard, Status, Top Sources, Top Destinations, Top Applications, Traffic History, Threat History, Network, Interfaces (highlighted), DNS, Config, Admin, Certificates, and Monitor. The main content area displays a table of interfaces.

Name	Type	IP/Netmask	Access	Administrative Status	Link Status
port1 (outside)	Physical	10.0.0.5 255.255.255.0	PING, HTTPS, SSH, FMG-Access	🟢	🟢 1000Mbps/Full Dup
port2 (inside)	Physical	10.0.1.5 255.255.255.0	PING, HTTPS, SSH	🟢	🟢 1000Mbps/Full Dup
port3	Physical	0.0.0.0 0.0.0.0		🟢	🔴
port4	Physical	0.0.0.0 0.0.0.0		🟢	🔴
port5	Physical	0.0.0.0 0.0.0.0		🟢	🔴
port6	Physical	0.0.0.0 0.0.0.0		🟢	🔴
port7	Physical	0.0.0.0 0.0.0.0		🟢	🔴
mesh.root (SSID: fortinet.mesh.root)	WiFi	0.0.0.0 0.0.0.0		🟢	

Step 6.3 – Setup basic policies

For this example we are going to create the following policies. (Samples below)

- NAT & allow outbound access
 - (Optional) You can apply any additional policies if you want to demonstrate features such as Web-filtering, DLP, etc.
- Port forwarding port 3389 to the Windows server
- Any required logging for troubleshooting

```
config firewall policy
  edit 1
    set srcintf "port2"
    set dstintf "port1"
    set srcaddr "all"
    set dstaddr "all"
    set action accept
    set schedule "always"
    set service "ALL"
    set utm-status enable
    set logtraffic all
    set av-profile "default"
    set ips-sensor "default"
    set profile-protocol-options "default"
    set nat enable
  next
```



```
edit 2
    set srcintf "port1"
    set dstintf "port2"
    set srcaddr "all"
    set dstaddr "Windows-RDP"
    set action accept
    set schedule "always"
    set service "ALL"
    set utm-status enable
    set logtraffic all
    set av-profile "AV-flow"
    set ips-sensor "default"
    set profile-protocol-options "default"
next
end

config firewall vip
    edit "Windows-RDP"
        set extintf "port1"
        set portforward enable
        set mappedip 10.0.1.25
        set extport 3389
        set mappedport 3389
    next
end
```

Step 7 – Testing

Step 7.1 – Launch a RDP session to test

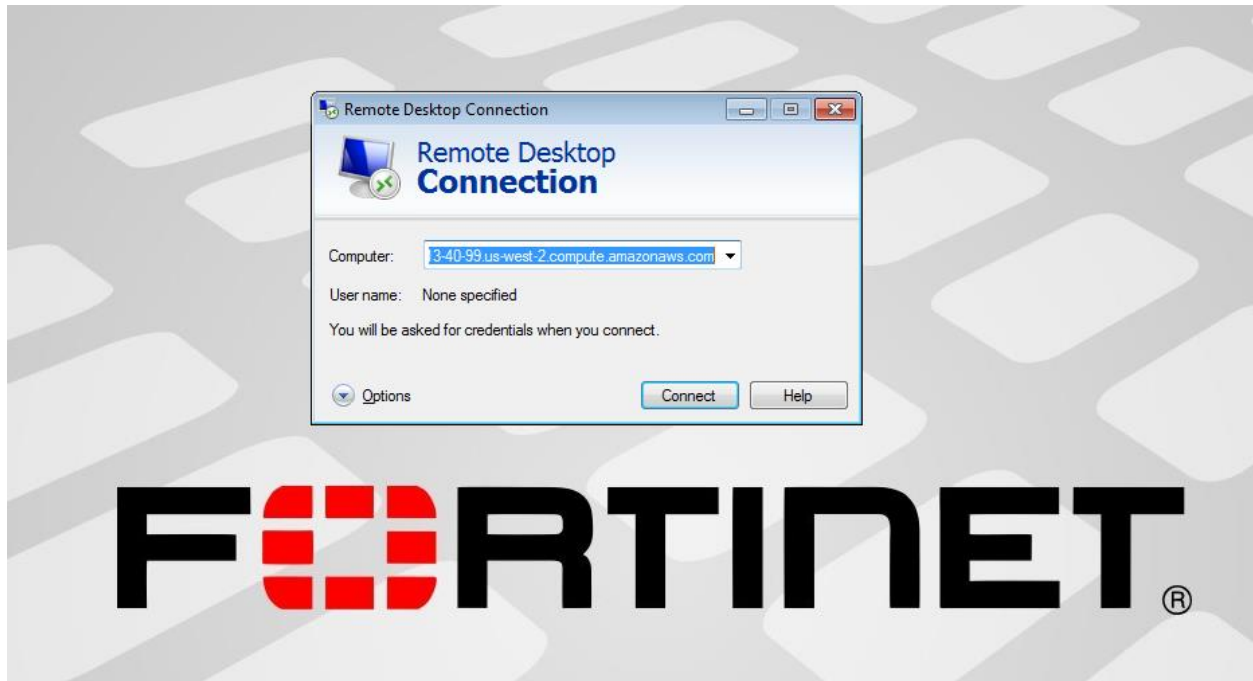


Figure 31

Step 7.2 – Retrieve your VM's password

On the EC2 Dashboard, Right click your test VM instance and select Get Windows Password

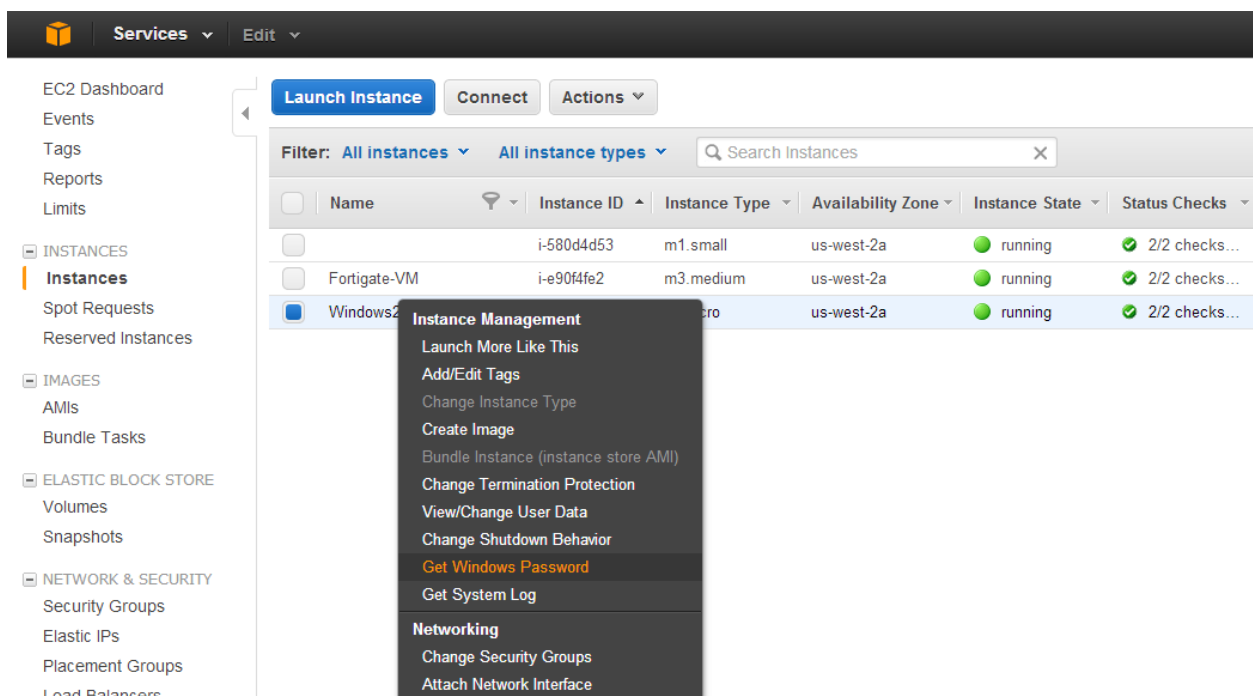


Figure 32

- You will be asked for the key pair you created to decrypt the administrator password.

Retrieve Default Windows Administrator Password

To access this instance remotely (e.g. Remote Desktop Connection), you will need your Windows Administrator password. A default password was created when the instance was launched and is available encrypted in the system log.

To decrypt your password, you will need your key pair for this instance. Browse to your key pair, or copy and paste the contents of your private key file into the text area below, then click Decrypt Password.

The following Key Pair was associated with this instance when it was created.

Key Name justinkey01

In order to retrieve your password you will need to specify the path of this Key Pair on your local machine:


Key Pair Path No file chosen


Or you can copy and paste the contents of the Key Pair below:

Paste contents of private key file here

Figure 33

Retrieve Default Windows Administrator Password

 **Password Decryption Successful**
The password for instance i-fa1959f1 (Windows2012-Test01) was successfully decrypted.

 **Password change recommended**
We recommend that you change your default password. Note: If a default password is changed, it cannot be retrieved through this tool. It's important that you change your password to one that you will remember.

You can connect remotely using this information:

Private IP	10.0.1.25
User name	Administrator
Password	k(nac;=K@w&

Step 7.3 – Test Outbound access

For testing purposes I have attempted to download a file from eicar.org to show that the FortiGate is inline for outbound traffic. See Figures 34-35.

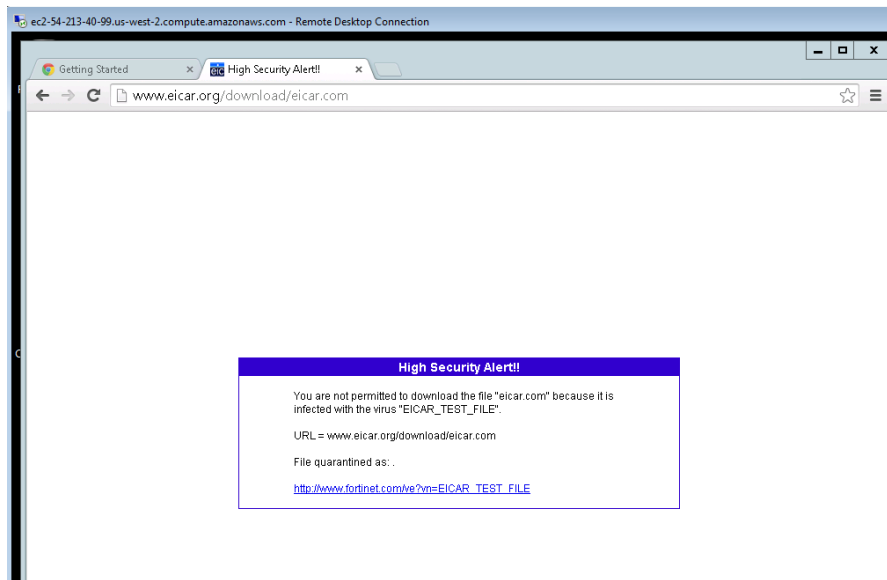


Figure 34

FortiGate VM64-AWS

Log location: D

#	Date/Time	Source	Device	Destination	Application Name	Security Action	Sent / Received	Application Details	Threat
1	15:24:18	10.0.1.25		188.40.238.250	Unknown		228 B / 132 B		
2	15:24:18	10.0.1.25		188.40.238.250	Unknown		228 B / 132 B		
3	15:24:18	10.0.1.25		188.40.238.250	Unknown		1.60 KB / 683 B		
4	15:24:18	10.0.1.25		188.40.238.250	Unknown		1.59 KB / 662 B		
5	15:24:18	10.0.1.25		188.40.238.250	Unknown		1.58 KB / 662 B		
6	15:24:18	10.0.1.25		188.40.238.250	Unknown		2.29 KB / 1.00 KB		
7	15:24:18	10.0.1.25		188.40.238.250	Unknown		920 B / 409 B		
8	15:24:18	10.0.1.25		188.40.238.250	Unknown		2.46 KB / 1.01 KB		
9	15:24:07	10.0.1.25		188.40.238.250	Unknown	✗	2.91 KB / 2.23 KB		EICAR_TEST_FILE
10	15:24:07	10.0.1.25		173.194.33.41	HTTP.BROWSER		630 B / 773 B		
11	15:23:49	10.0.1.25		173.194.33.103	Unknown		655 B / 855 B		

Application Details

Field	Value	Field	Value
Date/Time	15:24:07 (1408029847)	Destination Country	Germany
Destination	188.40.238.250	Dst Port	80
Dst Interface	port1	File Name	eicar.com
Duration	19	Level	notice
Hostname	www.eicar.org	Policy ID	1
Log ID	13	Received	2280
Protocol	6	Security Action	✗
Received Packets	11	Sent	2977
Security Event	virus	Sent Packets	11
Sent / Received	2.91 KB / 2.23 KB	Service	HTTP
Sequence Number	349	Source Country	Reserved
Source	10.0.1.25	Src NAT IP	10.0.0.5
Src Interface	port2	Src Port	49241
Src NAT Port	49241	Sub Type	forward
Status	close	Timestamp	8/14/2014 3:24:07 PM
Threat	EICAR_TEST_FILE	Virtual Domain	root
Tran Display	snat	Virus ID	2172
Virus	EICAR_TEST_FILE		

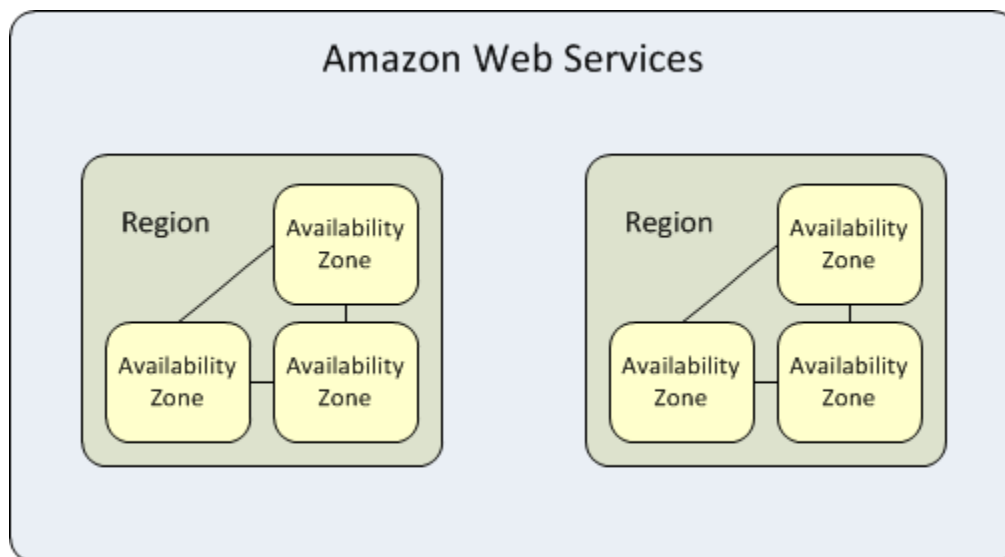
Figure 35

Appendix

Regions and Availability Zones

Region and Availability Zone Concepts

Each region is completely independent. Each Availability Zone is isolated, but the Availability Zones in a region are connected through low-latency links. The following diagram illustrates the relationship between regions and Availability Zones.



You can list the Availability Zones that are available to your account. For more information, see [Describing Your Regions and Availability Zones](#). When you launch an instance, you can select an Availability Zone or let us choose one for you. If you distribute your instances across multiple Availability Zones and one instance fails, you can design your application so that an instance in another Availability Zone can handle requests.

Amazon EC2 resources are either global, tied to a region, or tied to an Availability Zone. For more information, [see AWS documentation for the complete article](#).

Amazon EC2 Key Pairs

Amazon EC2 uses public-key cryptography to encrypt and decrypt login information. Public-key cryptography uses a public key to encrypt a piece of data, such as a password, then the recipient uses the private key to decrypt the data. The public and private keys are known as a *key pair*.

To log in to your instance, you must create a key pair, specify the name of the key pair when you launch the instance, and provide the private key when you connect to the instance. Linux/Unix instances have no password, and you use a key pair to log in using SSH. With Windows instances, you use a key pair to obtain the administrator password and then log in using RDP.

Creating a Key Pair

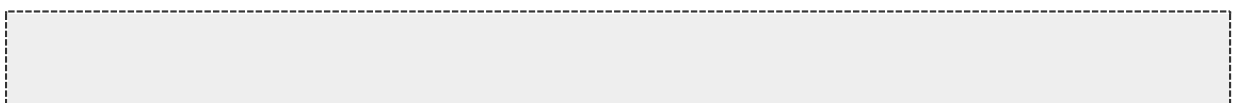
You can use Amazon EC2 to create your key pair. For more information, see [Creating Your Key Pair Using Amazon EC2](#). Alternatively, you could use a third-party tool and then import the public key to Amazon EC2. For more information, see [Importing Your Own Key Pair to Amazon EC2](#).

Each key pair requires a name. Be sure to choose a name that is easy to remember. Amazon EC2 associates the public key with the name that you specify as the key name. Amazon EC2 stores the public key only, and you store the private key. Anyone who possesses your private key can decrypt your login information, so it's important that you store your private keys in a secure place.

The keys that Amazon EC2 uses are 1024-bit SSH-2 RSA keys. You can have up to five thousand key pairs per region.

Launching and Connecting to Your Instance

When you launch an instance, you should specify the name of the key pair you plan to use to connect to the instance. If you don't specify the name of an existing key pair when you launch an instance, you won't be able to connect to the instance. When you connect to the instance, you must specify the private key that corresponds to the key pair you specified when you launched the instance. Amazon EC2 doesn't keep a copy of your private key; therefore, if you lose your private key, there is no way to recover it. If you lose the private key for an instance store-backed instance, you can't access the instance; you should terminate the instance and launch another instance using a new key pair. If you lose the private key for an EBS-backed instance, you can regain access to your instance. For more information, see [Connecting to Your Instance if You Lose Your Private Key](#).



Detailed VPC Diagram

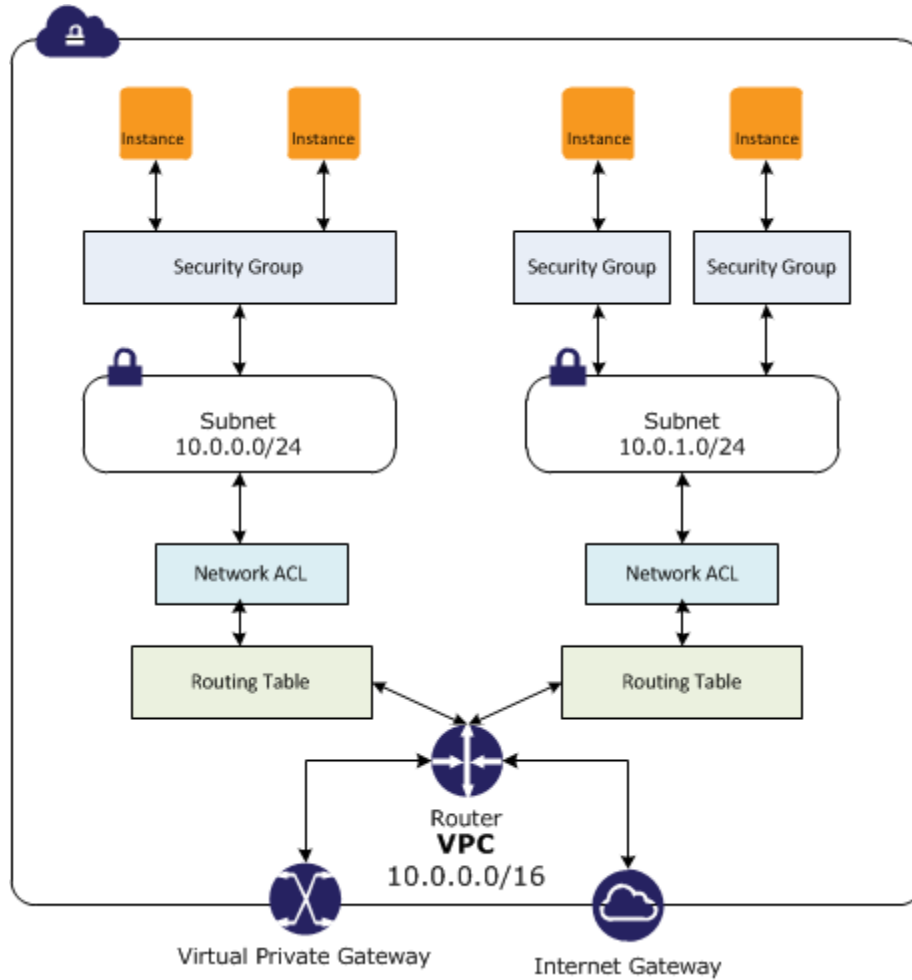


Figure 36

Additional info and links

<http://aws.amazon.com/documentation/vpc/>

http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Introduction.html